The above system provides a proof of submission and proof of delivery technique that employs a third party key provider. It should be understood that the implementation of other variations and modifications of the invention in its various aspects will be apparent to those of ordinary skill in the art, and that the invention is not limited by the specific embodiments described. For example, it will be recognized that if the third party public key is of sufficient length, then the security token 46 may be encrypted directly using the third party public key. Also, the operations of the various units may be performed by other units. For example, the key request reply 26 and the verifier 57 can be moved to the third party and the third party transfers the token 46 to the recipient processor to facilitate distributed processing. It is therefore contemplated to cover by the present invention, any and all modifications, variations, or equivalents that fall within the spirit and scope of the basic underlying principles disclosed and claimed herein.

Claims

What Is Claimed Is:

Sub B1

~~1. A method for securely communicating data comprising the steps of:~~

~~(a) providing, by a first party, a double key package to a second party;~~

~~(b) communicating, by the second party, the double key package to a third party; and~~

~~(c) decrypting, in part, the double key package to recover a decryption key for the second party using a third party based decryption key to facilitate mandatory communication between the second party and the third party and decryption of data based on the recovered decryption key.~~

~~2. The method of claim 1 including the steps of:~~

~~receiving the double key package by the second party; and~~

~~communicating the recovered decryption key package to the second party.~~

~~3. The method of claim 1 wherein the double key package includes the decryption key that is used to decrypt the encrypted data protected through a double application of asymmetric public key encryption.~~

B' amt

~~4. The method of claim 3 wherein the decryption key is a symmetric key and wherein the double application of asymmetric public key encryption is performed using a public key associated with the second party while another application of asymmetric public key encryption uses a public key associated with the third party.~~

Sub C'

~~5. The method of claim 1 in including the steps of:~~

~~generating cipher text by encrypting data with a first cryptographic key (Ks1) by the first party;~~

~~providing the cipher text to the second party;~~

~~encrypting the cryptographic key (Ks1) using a second encryption key associated with the second party to produce a first key package; and~~

~~encrypting the first key package using a third encryption key associated with the third party to the produce a double key package.~~

~~6. The method of claim 1 in including the steps of:~~

~~generating cipher text by encrypting data with a first cryptographic key (Ks1) by the first party;~~

~~providing the cipher text to the second party;~~

~~encrypting the cryptographic key (Ks1) using a second encryption key associated with the second party to produce a first key package;~~

~~encrypting the first key package using a third encryption key associated with the third party to the produce an encrypted first key package; and~~

~~encrypting the third encryption key with a fourth encryption key associated with the third party to produce a second key package,~~

~~wherein the double key package includes the second key package and the encrypted first key package.~~

~~7. The method of claim 6 wherein the first cryptographic key is a symmetric key, the second encryption key is an asymmetric public key, the third encryption key is a symmetric key and the fourth encryption key is an asymmetric public key.~~

B1 cont

~~8. The method of claim 1 including the step of recording, by the third party, receipt of the double key package from the second party to facilitate message data delivery tracking.~~

~~9. The method of claim 7 including the steps of:~~

~~generating message delivery status data, by the third party, in response to a signed status request;~~

~~processing the signed status request by verifying a digital signature on the signed request; and~~

~~determining authorization of a party seeking the request based on identification data obtained from the signed request.~~

~~10. A method for securely communicating data comprising the steps of:~~

~~(a) providing, by a first party, message data and a double key package to a third party;~~

~~(b) providing, by the third party, the message data and the double key package to a second party;~~

~~(c) receiving back from the second party, by the third party, the double key package;~~

~~(d) decrypting, in part, the double key package using a third party decryption key to recover a decryption key for the second party to provide mandatory communication between the second party and the third party; and~~

~~(e) communicating the recovered decryption key package to the second party to enable decryption of the message data by the second party.~~

11. The method of claim 10 including the step of providing time stamp data by the third party to the first party based on receipt of the message data and the double key package.

Sub a2

12. The method of claim 10 in including the steps of:

generating cipher text by encrypting data with a first cryptographic key (Ks1) by the first party;

providing the cipher text to the second party;

encrypting the cryptographic key (Ks1) using a second encryption key associated with the second party to produce a first key packaging; and

encrypting the first key package using a third encryption key associated with the third party to the produce a double key package.

B1 omit

13. The method of claim 10 in including the steps of:

generating cipher text by encrypting data with a first cryptographic key (Ks1) by the first party;

providing the cipher text to the second party;

encrypting the cryptographic key (Ks1) using a second encryption key associated with the second party to produce a first key package;

encrypting the first key package using a third encryption key associated with the third party to the produce an encrypted first key package; and

encrypting the third encryption key with a fourth encryption key associated with the third party to produce a second key package,

wherein the double key package includes the second key package and the encrypted first key package.

14. The method of claim 13 wherein the first cryptographic key is a symmetric key, the second encryption key is an asymmetric public key, the third encryption key is a symmetric key and the fourth encryption key is an asymmetric public key.

~~15. The method of claim 10 including the step of recording, by the third party, receipt of the double key package from the second party to facilitate message data delivery tracking.~~

B1 cont

~~16. The method of claim 10 including the steps of:~~

~~generating message delivery status data, by the third party, in response to authorized status request data;~~

~~processing the authorized status request by verifying the authorized request; and~~

~~determining authorization of a party seeking the request based on identification data obtained from the authorized request.~~

~~17. The method of claim 16 wherein the authorized request is a signed request.~~

~~18. An apparatus for securely communicating data comprising:~~

~~a first party cryptographic engine, operatively coupled to receive data for encryption, and adapted to produce a double key package wherein the double key package includes a decryption key that is used to decrypt the encrypted data protected through a double application of asymmetric public key encryption; and~~

~~a combiner, operatively coupled to combine the double key package with the cipher text.~~

B1 omit

~~19. The apparatus of claim 18 wherein the first party cryptographic engine generates cipher text by encrypting the data with a first cryptographic key (Ks1) , encrypts the first cryptographic key (Ks1) using a second encryption key associated with a second party to produce a first key package, and encrypts the first key package using a third encryption key associated with a third party to the produce the double key package.~~

~~20. The apparatus of claim 19 including a digital signor that applies a digital signature associated with a first party to at least one of the double key package and the cipher text to produce a signed message with a third party based encrypted security token.~~

~~21. The apparatus of claim 18 including:~~

~~a delivery status request generator that generates authorized proof of delivery request data for the third party;~~

~~a proof of delivery analyzer operatively coupled to receive proof of delivery data based on third party receipt of the double key package and the authorized delivery request data, and~~

~~a request verifier operative to verify authorization data associated with the proof of delivery data.~~

~~22. The apparatus of claim 21 wherein the authorization data includes digital signature data.~~

~~23. An apparatus for securely communicating data comprising:~~

~~a double key package evaluator wherein the double key package is generated by a first party; and~~

~~a double key package decryptor that partially decrypts the double key package to recover a decryption key package for a second party using a third party based decryption key to facilitate mandatory communication between the second party and the third party and decryption of data based on the recovered decryption key.~~

B1 cont

~~24. The apparatus of claim 23 wherein the double key package decryptor communicates the recovered decryption key package to the second party.~~

~~25. The apparatus of claim 24 including a time stamp generator providing time stamp data to the first party based on receipt of message data and the double key package from a second party.~~

~~26. The apparatus of claim 23 a time stamp generator providing time stamp data to the second party indicating when the first party sent message data to the third party.~~

~~27. An apparatus for securely communicating data comprising:~~

~~a first party cryptographic engine, operatively coupled to receive data for encryption, and adapted to produce a double key package wherein the double key package includes a decryption key that is used to decrypt the encrypted data protected through a double application of asymmetric public key encryption;~~

~~a combiner, operatively coupled to combine the double key package with the cipher text;~~

~~a double key package evaluator; and~~

~~a double key package decryptor that partially decrypts the double key package to recover a decryption key package for a second party using a third party based decryption key to facilitate mandatory communication between the second party and the third party and decryption of data based on the recovered decryption key.~~

B' cont

~~28. The system of claim 27 including a digital signor that applies a digital signature associated with a first party to the double key package and the cipher text to produce a signed message with a third party based encrypted security token.~~

~~29. The apparatus of claim 27 including:~~

~~a delivery status request generator that generates authorized delivery request data for the third party;~~

~~a proof of delivery analyzer operatively coupled to receive proof of delivery data based on third party receipt of the double key package and the authorized delivery request data, and~~

~~a verifier operative to verify the proof of delivery data.~~

~~30. The apparatus of claim 29 wherein the double key package decryptor communicates the recovered decryption key package to the second party.~~

B1 omit

~~31. The apparatus of claim 30 including a time stamp generator providing time stamp data to the first party based on receipt of message data and the double key package from a second party.~~

32. A storage medium containing data representing executable instructions comprising:

first memory containing data representing executable instructions that cause a processing device to provide, by a first party, a double key package to a second party;

second memory containing data representing executable instructions that cause a processing device to communicate the double key package to a third party; and to partially decrypt the double key package to recover a decryption key for the second party using a third party based decryption key package to facilitate mandatory communication between the second party and the third party and decryption of data based on the recovered decryption key.

B1 amt

33. The storage medium of claim 32 including data representing executable instructions that cause a processing device to receive the double key package by the second party; and communicate the recovered decryption key package to the second party.

Sub A3

34. The storage medium of claim 32 including data representing executable instructions that cause a processing device to

35. The storage medium of claim 32 including data representing executable instructions that cause a processing device to:

generate cipher text by encrypting data with a first cryptographic key (Ks1) by the first party;

provide the cipher text to the second party;

encrypt the cryptographic key (Ks1) using a second encryption key associated with the second party to produce a first key package; and

encrypt the first key package using a third encryption key associated with the third party to the produce a double key package.

~~36. The storage medium of claim 32 including data representing executable instructions that cause a processing device to provide the double key package to include the decryption key that is used to decrypt the encrypted data protected through a double application of asymmetric public key encryption.~~

B1 omit

~~37. The storage medium of claim 36 wherein the decryption key is a symmetric key and wherein the double application of asymmetric public key encryption is performed using a public key associated with the second party while another application of asymmetric public key encryption uses a public key associated with the third party.~~

~~38. The storage medium of claim 32 including data representing executable instructions that cause a processing device to record, by the third party, receipt of the double key package from the second party to facilitate message data delivery tracking.~~

~~39. The storage medium of claim 32 including data representing executable instructions that cause a processing device to generate message delivery status data, by the third party, in response to a signed status request; process the signed status request by verifying a digital signature on the signed request; and determine authorization of a party seeking the request based on identification data obtained from the signed request.~~

~~40. A method for securely communicating data comprising the steps of:~~

~~(a) providing, by a first party, a double key package to a second party;~~

~~(b) communicating, by the second party, the double key package to a third party; and~~

~~(c) decrypting, in part, the double key package to recover a decryption key package for the second party using a third party based decryption key to facilitate mandatory communication between the second party and the third party and decryption of data based on the recovered decryption key.~~

B1 omit

~~41. The method of claim 40 including the steps of:~~

~~receiving the double key package by the second party; and~~

~~communicating the recovered decryption key package to the second party.~~

~~42. The method of claim 40 wherein the double key package includes the decryption key that is used to decrypt the encrypted data protected through a double application of asymmetric public key encryption.~~

~~43. The method of claim 42 wherein the decryption key is a symmetric key and wherein the double application of asymmetric public key encryption is performed using a public key associated with the second party while another application of asymmetric public key encryption uses a public key associated with the third party.~~

~~44. The method of claim 40 in including the steps of:~~

~~generating cipher text by encrypting data with a first cryptographic key (Ks1) by the first party;~~

~~providing the cipher text to the second party;~~

~~encrypting the cryptographic key (Ks1) using a second encryption key associated with the second party to produce a first key package; and~~

~~encrypting the first key package using a third encryption key associated with the third party to the produce a double key package.~~

B1 am't

~~45. The method of claim 40 in including the steps of:~~

~~generating cipher text by encrypting data with a first cryptographic key (Ks1) by the first party;~~

~~providing the cipher text to the second party;~~

~~encrypting the cryptographic key (Ks1) using a second encryption key associated with the second party to produce a first key package;~~

~~encrypting the first key package using a third encryption key associated with the third party to the produce an encrypted first key package; and~~

~~encrypting the third encryption key with a fourth encryption key associated with the third party to produce a second key package,~~

~~wherein the double key package includes the second key package and the encrypted first key package.~~

~~46. The method of claim 45 wherein the first cryptographic key is a symmetric key, the second encryption key is an asymmetric public key, the third encryption key is a symmetric key and the fourth encryption key is an asymmetric public key.~~

~~47. The method of claim 40 including the step of recording, by the third party, receipt of the double key package from the second party to facilitate message data delivery tracking.~~